SIN 471

Issue 3.10

July 2023

Suppliers' Information Note

For The BT Network

BT Wholesale Broadband Managed Connect Shared

Service Description

Each SIN is the copyright of British Telecommunications plc. Reproduction of the SIN is permitted only in its entirety, to disseminate information on the BT Network within your organisation. You must not edit or amend any SIN or reproduce extracts. You must not remove BT trademarks, notices, headings or copyright markings.

This document does not form a part of any contract with BT customers or suppliers.

Users of this document should not rely solely on the information in this document, but should carry out their own tests to satisfy themselves that terminal equipment will work with the BT network.

BT reserves the right to amend or replace any or all of the information in this document.

BT shall have no liability in contract, tort or otherwise for any loss or damage, howsoever arising from use of, or reliance upon, the information in this document by any person.

Due to technological limitations, a very small percentage of customer interfaces may not comply with some of the individual characteristics, which may be defined in this document.

Publication of this Suppliers' Information Note does not give or imply any licence to any intellectual property rights belonging to British Telecommunications plc or others. It is your sole responsibility to obtain any licences, permissions or consents which may be necessary if you choose to act on the information supplied in the SIN.

Those BT services marked ® indicates it is a registered trademark of British Telecommunications plc.
Those BT services marked ™ indicates it is a trademark of British Telecommunications plc.

This SIN is available in Portable Document Format (pdf) from: https://www.bt.com/about/sinet

Enquiries relating to this document should be directed to: sinet.helpdesk@bt.com

© British Telecommunications plc
Registered Office 1 Braham Street LONDON E1
Registered in England no.1800000

CONTENTS

1 INTRODUCTION 4

2 AVAILABILITY 5

3 SERVICE OUTLINE 6

4 BT WBMC SHARED (AGGREGATED) SERVICE 7

- 4.1 GENERAL 7
- 4.2 FEATURES OF THE SHARED AGGREGATION PRODUCT 8
  - *4.2.1 Available Contracted Bandwidths and traffic classes 9*
  - *4.2.2 Connectivity to the CPs network and Routing updates 11*
  - *4.2.3 Autonomous System (AS) Numbers 13*
  - *4.2.4 Direction of sessions at end user login 14*
    - 4.2.4.1 General 14
    - 4.2.4.2 Service Selection Name Options 14
    - 4.2.4.3 Presentation of Service Selection Name 15
    - 4.2.4.4 Username and Service Selection Name length 16
  - *4.2.5 WBC-Specific Session Handling Information 16*
    - 4.2.5.1 WBC Session Handling under failure 16
    - 4.2.5.2 WBC FTTC PPP Session Timeouts 17
  - *4.2.6 IPsC-Specific Session Handling Information 17*
    - 4.2.6.1 IPsC Session Handling under failure 17
- 4.3 RADIUS INTERFACE DETAIL 17
  - *4.3.1 General 17*
  - *4.3.2 Differentiating between IPsC & WBC RADIUS traffic 19*
    - 4.3.2.1 Agnostic Approach (Recommended) 19
    - 4.3.2.2 Differentiating between service types 19
  - *4.3.3 RADIUS Interface for WBC End Users 20*
    - 4.3.3.1 WBC End User Authentication and Tunnel Selection 20
    - 4.3.3.2 WBC End User RADIUS Accounting 21
  - *4.3.4 RADIUS Interface for IPsC End Users 23*
    - 4.3.4.1 IPsC End User RADIUS Authentication 23
    - 4.3.4.2 IPsC End User RADIUS Accounting 26
- 4.4 WBMC SHARED TRAFFIC TYPES 28

5 REFERENCES 29

6 ABBREVIATIONS 30

7 HISTORY 33

FIGURES

Figure 1 – Positioning of WBMC 6

Figure 2 – WBMC Shared Network Structure 8

TABLES

Table 1 Access-Request Attributes for WBMC Shared over WBC 20

Table 2 Access-Reject Attributes for WBMC Shared over WBC 21

Table 3 L2TP Access-Accept Attributes for WBMC Shared over WBC 21

Table 4 Accounting Attributes for WBMC Shared over WBC 22

Table 5 Accounting-Response Attributes for WBMC Shared over WBC 22

Table 6 Access Request Attributes for WBMC Shared over IPsC 23

Table 7 Access Accept Attributes for WBMC Shared over IPsC 25

Table 8 RADIUS Accounting Attributes for WBMC Shared over IPsC 27

Table 9 DSCP Markings 28

1 Introduction

This SIN covers Wholesale Broadband Managed Connect (WBMC) Shared. It describes the service for WBMC Shared over Wholesale Broadband Connect (WBC) and IPstream Connect (IPsC).

Please see the Customer Handbook for an end-to-end service description, available product options, ordering, fault management, migration, billing and commercial details. This is available at:

https://www.btwholesale.com/pages/static/products-services/wholesale-broadband-managed-connect.htm

Definitions:

For the purposes of this document the following definitions apply:

Communication Provider (CP): The Service Provider (SP) or Business Customer (BC) who purchases the WBMC Shared service from BT Wholesale and sells or provides it to End-Users.

End User (EU): The person using their device to connect to a SP/BC's IP network via the BT WBMC Shared service.

WBMC Shared Backhaul: An instance of the WBMC Shared service, which consists of three components:

- a bandwidth component, detailing how much bandwidth the CP is able to send and receive from the BTW network across that specific WBMC Shared backhaul service instance
- a Host Link component, providing physical connectivity between a single BTW node and a single Communications Providers network
- the MPLS Network

This document should be read in conjunction with the following SINs for the WBC service:

- SIN 472 [7] - BT Wholesale Broadband Connect Service Description;
- SIN 495 [16] - BT Wholesale Broadband Connect Fibre to the Cabinet Service. This SIN is appropriate if the CP is supporting WBC FTTC End User Access. For FTTC, please also refer to the Openreach SIN for FTTC Generic Ethernet Access (SIN 498 [19]) which covers the End User equipment interface details;
- SIN 509 [22] – BT Wholesale Broadband Connect (WBC) Fibre to the Premise (FTTP) Service & Interface Description. This SIN is appropriate if the CP is supporting WBC FTTP End User Access. Please also refer to the Openreach SINs for FTTP Generic Ethernet Access (SIN 506 [21]).

This document should be read in conjunction with the following SINs for the IPstream Connect service:

- SIN 482 [9] - BT IPstream Connect Service Description;
- SIN 485 [11] - BT IPstream Connect Office, BT IPstream Connect Home, BT IPstream Connect Max & BT IPstream Connect Max Premium Products;
- SIN 487 [14] - BT IPstream Connect Symmetric. This SIN is appropriate if the CP intends to offer SDSL End User services;
- SIN 496 [17] - BT IPstream Connect SID for Authentication;
- SIN 497 [18]- BT IPstream Connect SID for Accounting;
- SIN 502 [20] – BT IPstream Connect Session Steering.

2 Availability

The WBMC Shared product is available within the following geographic footprint:

Customer Sited Handover:

- At 1Gbps, within the reach of a standard reach BT Openreach EAD product from the WBMC Shared Interconnect Nodes.
- At 10Gbps, within the reach of a standard reach BT Openreach EAD product from a subset of the WBMC Shared Interconnect Nodes.

In Building Handover:

- At 1Gbps, 10Gbps and 100Gbps within the WBMC Interconnect Node. The In Building Handover is provided using an Openreach Cablelink.

Third Party Datacentre:

- 10Gbps and 100Gbps connectivity is available from a limited number of third party Datacentres.

Notes:

1. Openreach EAD products are used for Customer Sited Handover Host Links. In Building Handover Host Links at the WBMC Shared Interconnect Node are also available via an Openreach Cablelink
2. We can provide hand-off at a subset of the Datacentres (Telehouses) when connecting to a subset of the WBMC Shared Interconnect Nodes. This will not affect the geographic coverage of WBMC Shared.

The Metro Node Connectivity increases the number of interconnect nodes supported for 1Gbps Customer Sited Handover. Please refer to the WBMC Customer Handbook for an up-to-date list of available nodes.

See SIN 492 [15] for EAD and SIN 519 for 10G EAD [23], available at sinet.helpdesk@bt.com.

WBC FTTC & FTTP end user coverage is subject to Openreach's rollout plans. WBMC Shared will support all WBC End User Access technologies in accordance with their published plans. Please check the availability with your BT Account Manager, or refer to the following websites:

- For WBC ADSL & Fibre availability information, please see the "21C Broadband Service Availability & Network Inventory" section at https://www.btwholesale.com/pages/static/help-and-support/network-information.htm;

3 Service Outline

The WBMC Shared Service provides connectivity between the WBC End User Access products & IPstream Connect products and the CPs network. WBMC Shared may be used by a CP to provide connectivity to WBC ADSL, WBC FTTC, WBC FTTP, WBC SoGEA, IPstream Connect, or a combination of these products. The traffic for all products will be carried over the same customer Host Links.

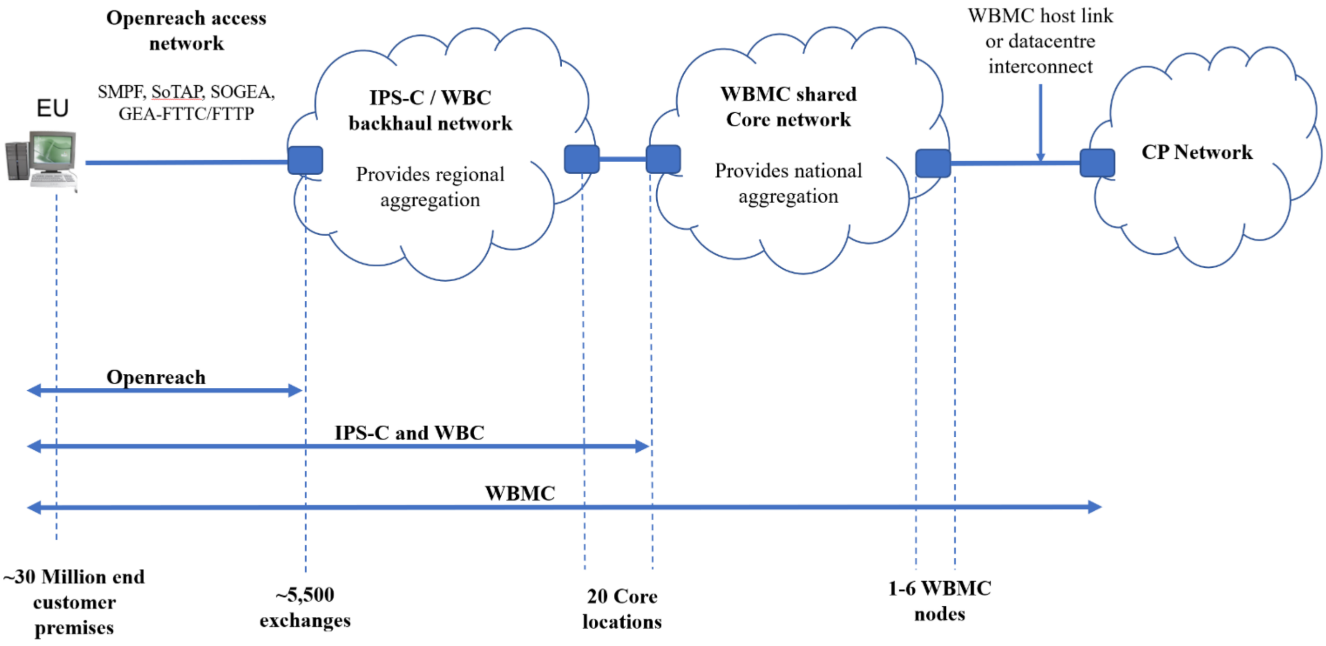
Openreach access network
SMPF, SoTAP, SOGEA, GEA-FTTC/FTTP
EU
IPS-C / WBC backhaul network
Provides regional aggregation
WBMC shared Core network
Provides national aggregation
WBMC host link or datacentre interconnect
CP Network
Openreach
IPS-C and WBC
WBMC
~30 Million end customer premises
~5,500 exchanges
20 Core locations
1-6 WBMC nodes

Figure 1 – Positioning of WBMC product alongside WBC and Openreach products

WBMC Shared is an end-to-end Broadband product. The positioning of WBMC Shared and the products it consumes is illustrated in Figure 1 above.

WBC ADSL & IPstream Connect are based on the Openreach Shared Metallic Path Facility (SMPF) which requires an underlying Openreach WLR service to be in place. WBC SOADSL offers similar ADSL2+ broadband functionality but is based on the Openreach SoTAP product. With each of these ADSL type products DSLAM/MSANs are located in BT Exchanges and connected to BRASes (Broadband Remote Access Servers) which are typically located in larger exchange buildings and core nodes. WBC supports ADSL2+ and includes ADSL2+ Annex M, which offers the possibility of greater upstream line rates by sacrificing some downstream line rate – see SIN 472 [7] for more details.

WBC FTTC & SOGEA End User Accesses differ in that they are based on the Openreach FTTC Generic Ethernet Access (GEA) product, which provides DSLAMs located in Street Cabinets and fibre from the Street DSLAMs to the BT Exchanges. WBC FTTC/SOGEA uses VDSL2 technology and allows higher bandwidths per End User compared with WBC (ADSL2+) & IPsC (ADSL1).

WBC FTTP End User Access is based on the Openreach FTTP Generic Ethernet Access (GEA) product. It offers an active wholesale network connection from the WBC Aggregation Point (AP) to the end user premise, with Ethernet presentation at the End User's Network Interfaces. CPs will be able to provide their broadband services over this active network connection.

WBC End User Access traffic is passed to WBMC Shared over a common WBC backhaul network i.e. traffic from all access types is eventually aggregated and mixed together on common infrastructure allowing for a single set of interconnects to service all WBC product types.

4 BT WBMC Shared (Aggregated) service

4.1 General

This service provides CPs with a means of accessing a Wholesale Broadband Connect (WBC) – ADSL, FTTC, SOGEA, FTTP & IPstream Connect (IPsC) end user base without the need to purchase interconnects at each of the WBC & IPsC interconnect nodes. A CP buys one or more WBMC Shared Backhauls as part of the WBMC Shared service. Each instance of backhaul represents a specific set of Host Links from a WBMC Shared Interconnect Node to the CPs network and an amount of bandwidth that the CP can send and receive over those Host Links. End user traffic from each of the WBC & IPsC nodes is carried in L2TP tunnels over a shared network to the WBMC Shared Interconnect Nodes. Please refer to the WBMC Customer Handbook for an up-to-date list of available WBMC Shared Interconnect Nodes. From a WBMC Shared Interconnect Node, the traffic is then delivered over the Host Links to the CPs network.

The delivery mechanism for these Host Links may be as follows:

- Customer Sited Handover, via either 1GE EAD products or 10G EAD, to the customer's premises;
- At a subset of the Datacentres (Telehouses), when connecting to a subset of the WBMC Shared Interconnect Nodes, BT-provided DWDM transmission will be used to deliver the Host Links rather than EAD;
- In Building Handover via BT Openreach CableLink to customer accommodation in the WBMC Shared Interconnect Node.

There will be differences in the provisioning mechanism for each option, which will be reflected in the WBMC Shared CRF.

There is a maximum number of 32 physical links (16 resilient 1G, 10G or 100G pairs) per WBMC Shared Backhaul purchased. A CP can choose to buy just a single WBMC Shared backhaul to provide connectivity to all WBC/IPsC interconnect points and all of their WBC (ADSL, FTTC, SOGEA and FTTP) & IPsC end users nationwide.

Customers shouldn't mix 1G, 10G and 100G Host Links at the same WBMC Interconnect Node. Also, we do not recommend mixing 1G,10G and 100G Host Links between WBMC interconnect Nodes. **Should a Customer wish to mix 1G, 10G and 100G Host Links then they must ensure they control traffic by advertising different prefixes over the BGP peers for the 1G, 10G and 100G Host Links. Failure to do this will result in the discarding of traffic**.

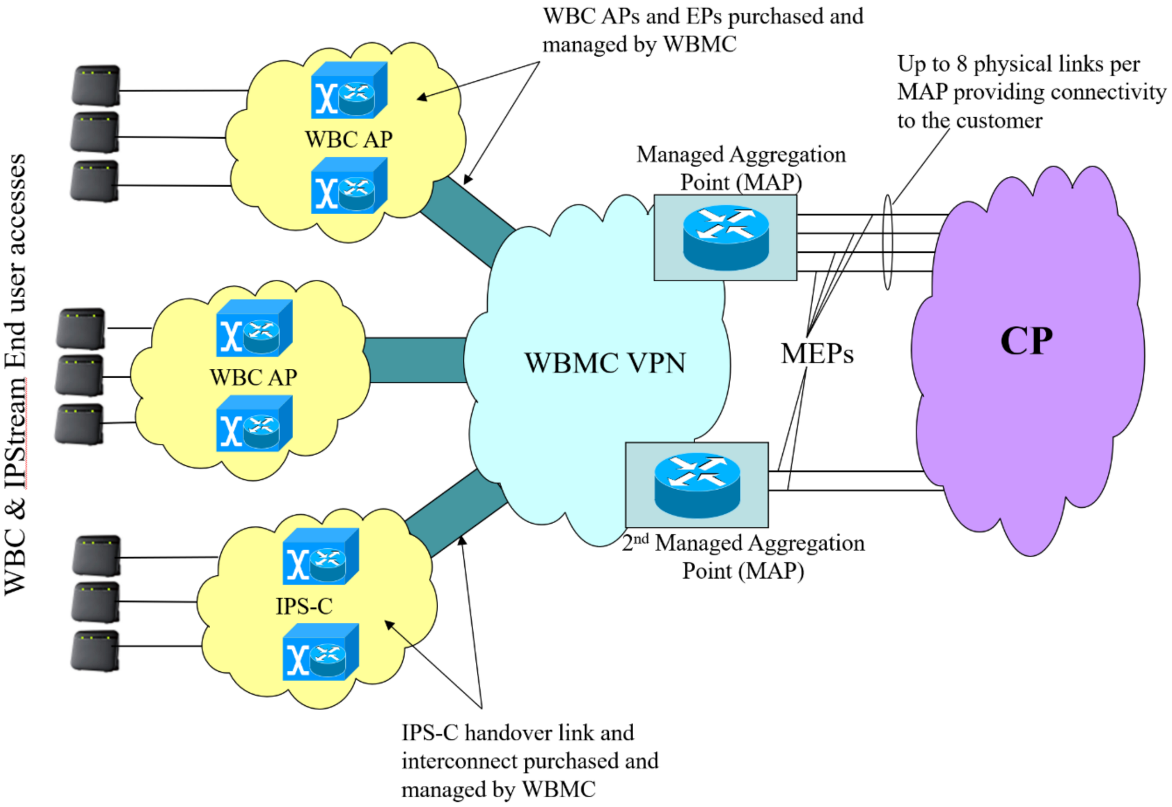
WBC APs and EPs purchased and managed by WBMC
Up to 8 physical links per MAP providing connectivity to the customer
Managed Aggregation Point (MAP)
WBC AP
WBC AP
IPS-C
WBMC VPN
MEPs
CP
2nd Managed Aggregation Point (MAP)
IPS-C handover link and interconnect purchased and managed by WBMC
WBC & IPStream End user accesses

Figure 2 – WBMC Shared Network Structure

The WBMC Shared service is only available in a PPP passthrough presentation option. With this option, PPP sessions are forwarded on to the CPs network within L2TP tunnels and it is the responsibility of the CP to terminate these PPP sessions and assign an IP address to the session. Note that there is no tunnel aggregation function within the WBMC Shared PPP passthrough service. The CPs network will receive a L2TP tunnel from each of the WBC & IPsC BRAS's to which their end users are connected.

4.2 Features of the Shared Aggregation product

4.2.1 Available Contracted Bandwidths and traffic classes

The WBMC Shared product aims to support the traffic classes available from the underlying products – WBC ADSL, WBC FTTC, WBC SOGEA, WBC FTTP and IPstream Connect.

At present, WBC Best Efforts, WBC Real Time & IPsC Best Efforts traffic is supported by WBMC Shared.

Notes:

1) WBC Real Time QoS applies to appropriately-marked traffic in both upstream and downstream directions. Please see SIN 472 for more details.

The sum total Contracted Bandwidth of the traffic classes requested on a WBMC Shared order cannot exceed the bandwidth of the physical links carrying the traffic from BTW's network to the CP. The product is sold and supported on the basis that the physical links are used as resilient pairs. The following Contracted Bandwidth options are available & apply to WBC and IPsC Best Efforts:

Bandwidth	Step size
1Mbps	1Mbps
2Mbps	
:	
:	
10Mbps	
12Mbps	2Mbps
:	
:	
50Mbps	
55Mbps	5Mbps
:	
:	
100Mbps	
110Mbps	10Mbps
:	
:	
500Mbps	
520Mbps	20Mbps
:	
:	

1Gbps	
1.05Gbps	50Mbps
:	
:	
2Gbps	
2.1Gbps	100Mbps
:	
:	
3.9Gbps	
4.03Gbps	134Mbps
:	
:	
8.6Gbps	
8.86Gbps	268Mbps
:	
:	
17.18Gbps	
17.72Gbps	536Mbps
:	
:	
34.36Gbps	
35.44Gbps	1.07G
:	
:	
39.73Gbps	
40Gbps	2G
:	
:	
400Gbps	

Notes:

1) 1Mbps = 1 Million bits per second

2) The bandwidth measurements for billing and policing are made at the Ethernet layer and include the Ethernet header, payload and trailer but do not include the pre-amble, start of frame delimiter or the interframe gap.

3) CPs are permitted to mark up to 5% of their contracted bandwidth as RTQoS for use with the WBC Real Time QoS service. If a CP attempts to send more than 5%, any excess traffic with the RTQoS marking will be dropped.

The WBMC Shared network will not police Best Efforts traffic to the contracted bandwidth. CPs will be able to fully utilise the port bandwidth if they choose to. It is the CPs responsibility to police the traffic to a contracted bandwidth level and any bandwidth used above the contracted level will be charged for appropriately.

For bandwidth & burst charges please see the WBMC Shared Terms and Conditions.

4.2.2 Connectivity to the CPs network and Routing updates

The CP will be provided with dedicated, WBMC-specific circuits to connect to the CPs network. BTW will provide a number of resilient circuits to meet the CPs requirements. All new 1G and 10G Customer Sited Handover Host Link orders are met using Openreach EAD. All In Building Handover Host Link orders are met using Openreach CableLink.

At a limited number of Datacentres (Telehouses) we can provide Host Link connectivity using BT supplied DWDM transmission, instead of Openreach EAD. The provisioning mechanism will have some differences, which will be reflected into the WBMC Shared CRF. The CRF will guide the CP to choose the correct option for their premises.

A mix of EAD, Transmission and In Building Handover cablelink based Host Links are supported on the same WBMC Shared service instance.

The product does not support a mix of 1G and 10G Host Links on the same WBMC Shared service instance. Customers wishing to move from 1G to 10G Host Links will be migrated to a new 10G service.

All Customer Sited Handover Host Links are provided using Resilience Option 2. For EAD delivery, Resilience Option 2 requires 2 EAD NTEs to be installed at the CPs premises. For DWDM transmission delivery to Datacentres (Telehouses), the BT delivery will terminate at a specified patch panel, and the CP will be responsible for connecting between their equipment and the BT patch panel.

The termination of both links at the CP premises must be in the same customer building; however the 2 links may be terminated in different rooms of the same building.

In Building Handover Host Links are provided using two Openreach CableLinks to the CPs accommodation in the WBMC Shared Interconnect Node.
Notes:

1) Subsequent orders to the same CP location will be provided on the same pair of CableLinks;
2) It is the CPs responsibility to obtain accommodation in the WBMC Shared Interconnect Node, provide rack space for the CableLink, and install the equipment needed to interface with WBMC Shared Host Links.

For rack, space and physical presentation details of the service delivered via 1G EAD please see the EAD SIN (SIN 492 [15]) and the EAD Product Description; for 10G EAD delivery please refer to the 10G EAD SIN (SIN 519 [23]) and EAD Product Description. For In Building Handover please refer to the Openreach CableLink Product Description. The SIN's are available from https://www.bt.com/about/sinet. The EAD & CableLink product documentation is available from the Openreach website.

Notes:

- The current resilient EAD product offerings do not offer guaranteed separacy of fibres but separacy is provided on a best endeavour's basis;
- For 1G Customer Sited Handover via EAD, the WBMC service currently only supports the Dual LC 1000BaseLX (Single Mode fibre) presentation option;
- Where 1G DWDM Transmission is utilised to Datacentres, the service uses Dual SC/PC 1000BaseLX (Single Mode fibre) presentation;
- For 1G In Building Handover, the service uses SC/APC 1000BaseLX (Single Mode Fibre) presentation;
- For 10G EAD Customer Sited Handover, the service uses the Dual LC 10GBase-LR (LAN-PHY) Single Mode fibre presentation option;
- Where 10G DWDM Transmission is utilised to Datacentres, the service uses Dual SC/PC 10GBase-LR (LAN-PHY) Single Mode fibre presentation;
- For 10G In Building Handover, the service uses SC/APC 10GBase-LR (LAN-PHY) Single Mode fibre presentation;
- The WBMC use of EAD will not utilise the User Link Loss Forwarding option.

The traffic will be presented to the CP within a VLAN. The same VLANs will carry both IPsC and WBC traffic types. Each bearer will have its own VLAN ID. BT will inform the CP of the VLAN IDs allocated during the provisioning process. BT will allocate VLAN IDs from the range 1006 to 1253 to each bearer, though if a VLAN ID clashes with an existing VLAN ID in use within the CPs network, the CP can request that the ID be changed (note that the new VLAN ID must also be in the range 1006 to 1253 and must not clash with a VLAN ID already in use).

For each physical link (2 per Host Link) connecting the CPs network to BT's network, an eBGP peering will be set-up between the BT network and the first Layer 3 CP device connected to the physical link. For each eBGP peering, a CP-provided RIPE public /30 address range is required.

The CP is advised not to place a L2 switch in front of the L3 device as this may compromise the availability of the service. WBMC recommends that the first networking device in the CPs network should terminate the Host Link layer 3 VLANs and the eBGP peering.

For all Host Link VLANs between the BT network and the CP, the CP should set their MTU size large enough to allow L2TP packets in the downstream direction without fragmentation. BT will use a MTU size of 1900 bytes on the VLANs. eBGP updates may be sent as 1900 byte packets, therefore the CP should ensure that there are no devices in their network that would prevent packets of that size.

At the point of ordering the service the CP will be asked to define a number of IP address ranges to associate with each eBGP peer. The address ranges must be public IP address ranges. They will be configured within an Access Control List (ACL) on the corresponding WBMC Shared device so that when the address range is advertised from the associated eBGP peer, the route can be accepted into the BTW network and traffic from the WBC & IPsC aggregation points can find its way to the correct device in the CPs network via the WBMC Shared Interconnect Node. WBMC will support up to 400 pre-agreed, separate prefixes (IP address ranges) per eBGP peer. BTW will reject routes advertised by the CP that have not previously been specified for that eBGP peer as part of a WBMC Shared Backhaul order.

For example, if the CP specifies the prefixes 10.16.164.0/29 & 10.16.164.8/29 on the CRF, and the CP advertises the prefix 10.16.164.4/32, this would not be allowed as it is not an agreed prefix. To work in this way the CP would need to specify the following prefixes:

- 10.16.164.0/29
- 10.16.164.4/32
- 10.16.164.8/29

It is permissible for the CP to plan ahead by informing BT when placing their order of prefixes for additional LNSes that they the plan to use in future. The CP may also add prefixes to their service at a later date using the WBMC CRF.

It is permissible for the CP to advertise the same prefixes out of multiple eBGP peers into the same WBMC Shared Interconnect Node. If the CP advertises the same prefixes from multiple eBGP peers associated with different WBMC Shared backhauls, BTW cannot guarantee the appropriate distribution of traffic across the backhauls.

WBMC will only allow prefixes that have a single AS number in the AS path list. Should a CP have a requirement to advertise prefixes with multiple AS numbers in the AS path list, this will be evaluated on a case by case basis.

Note: WBMC will not make any routing decisions based on the AS path length.

The CP may advertise MEDs (Multi-Exit Discriminators) alongside the address ranges via their eBGP peers into the WBMC Shared network. WBMC Shared will honour these route metrics and distribute the upstream traffic (from BTW's network to the CPs network) accordingly.

Note: MEDs will only work across eBGP peers associated with a single WBMC Shared service instance at a single interconnect node.

For downstream traffic, the CP may distribute the traffic across each Host Link into a WBMC Shared Interconnect Node as they see fit within the capacity of each of the bearers available and the Contracted Bandwidth for the various traffic classes purchased from WBMC Shared as part of the WBMC Shared Backhaul.

WBMC will advertise the IPsC and WBC BRAS tunnel end point IP addresses as individual /32's over the eBGP peers to CPs.

Note: The number of BRAS tunnel end point IP addresses being advertised could be up to 3000 at any one time.

4.2.3 Autonomous System (AS) Numbers

The CP must provide an Autonomous System (AS) Number when ordering their WBMC Shared service. The same AS Number will be used for all Host Links associated with a service instance.

The same AS Number may be used for multiple WBMC Shared service instances at the same or different interconnect nodes, however:

- The same AS number can support up to 16 Host Links at the same interconnect node, on the same or across different service instances. If more than 16 Host Links are provided from a single interconnect node then additional AS number(s) must be provided;
- If multiple Metro Node Connectivity service instances are required, it is possible under exceptional circumstances that separate AS numbers may need to be provided for each, even if the service instances handoff at different Metro Nodes. If this occurs the CP will be informed during the order process and asked to provide a second AS Number.

16 bit vs. 32 bit AS Numbers

The WBMC Shared product supports 16 bit and 32 bit AS numbers.

The preference is for CPs to use Public AS Numbers, however if this is not possible, CPs should propose a Private AS number which will need to be negotiated with WBMC to avoid a clash with another CP. **The AS number CPs need to peer with on WBMC is 65200. Also 2856, 65020, 65099, 65100 and 65400 are used within WBMC and as such all are unavailable to CPs.**

4.2.4 Direction of sessions at end user login

4.2.4.1 General

The CP will be required to support one tunnel per BRAS from within the WBC and/or IPsC network to each of the CPs specified tunnel end points – there is no tunnel aggregation function within the WBMC Shared product.

4.2.4.2 Service Selection Name Options

In order to allow a degree of flexibility in mapping end users into various end points or interconnects into the CPs network, WBMC Shared supports the use of Service Selection Names to appropriately direct the end users PPP session through the network based on the end user login details.

The same Service Selection Name (SSN) may be used for both the IPsC & WBC services over WBMC Shared. There is a limit of 50 Service Selection Names per CP in total. Requests for more than 50 Service Selection Names may be considered in exceptional circumstances – please discuss with your Account Manager.

Service Selection Names can be used in a variety of configurations as detailed below to achieve the desired distribution of the CPs end user base across the WBMC Shared service. The Service Selection Name is the last part of the text entered by the end user during the CHAP authentication process used within WBC, IPsC and WBMC.

Illustration:

> If an end user entered the username of joe.bloggs@WBMC.ISP.com, the text after the @ symbol constitutes the Service Selection Name, in this case WBMC.ISP.com

Where a range of tunnel end points is specified to BT, the CP can map Service Selection Name to tunnel end points in the following ways:

- One Service Selection Name to one tunnel end point
- One Service Selection Name to many tunnel end points (recommended for high availability of service)
- Many Service Selection Names to one tunnel end point
- Many Service Selection Names to many tunnel end points (recommended for high availability of service)

As stated above, the CP is required to advertise the tunnel end points into the BTW network. The CP can choose to advertise some tunnel end points associated with a SSN through one WBMC Shared Backhaul instance, and others associated with the same SSN through a different Backhaul instance. There is no restriction on SSN to Backhaul mapping, only SSN to tunnel end point mapping where a pre-configured list of tunnel end points is held in the WBMC Shared network against an SSN.

Where many tunnel end points are used, the CP should be advised that there is a limit of 400 IP addresses per Service Selection Name.

4.2.4.3 Presentation of Service Selection Name

This is how the username and Service Selection Name is presented to the CP in the RADIUS Access requests. There are two formats available, listed below.

Note: Where a Service Selection Name is used for both IPsC and WBC, the CP must ensure that the same presentation of the Service Selection Name is used for both services.

- **Default Service Selection Name**

  Two formats of presenting the Service Selection Name and user name are supported. These are:

  End.user@link.business-name.com

  Link.business-name.com/end.user

  Please note:

  - *The characters '/', '\', '%' '@', '!', '$' and '#' are reserved characters and can not be used within a username or domain name.*
  - *It is possible for CPs to receive "domain/user" even if they are expecting "user@domain". How this is processed is up to the CP.*

  The Virtual Service Selection Name option (presented below) is not compatible with the '/' delimiter Service Selection Name format.

- **Virtual Service Selection Names**

  This option will allow a portion of the username to be included in the Service Selection Name of the WBMC Shared service.

For example, a CP with a Service Selection Name of sp.com and an End User with a name of Fred Bloggs could have a login string of 'fred@bloggs.sp.com' and would have this string presented to their RADIUS.

This is primarily used for groups of End Users using multiple mailboxes from a single connection e.g. different first names for a family connection or employees with a company.

With Virtual Service Selection Names everything to the left of the first '.' in the Service Selection Name is treated as a wildcard, everything to the right of the first '.' is treated as the selecting Service Selection Name (the Service Selection Name entered on the End User CRF). Only a single string pre-pending the selecting Service Selection Name is allowed (i.e. '.' – may not be included), e.g. in:-

fred@bloggs.isp.com

"fred" is the username

"bloggs" is the wildcard

"isp.com" is the selecting domain name.

4.2.4.4 Username and Service Selection Name length

The maximum length of the combined username and Service Selection Name string can be no longer than 253 characters (including the separator).

The maximum length of a Service Selection Name is 32 characters (applies to everything to the right of the first '.' if the Virtual Service Selection Name option is selected).

4.2.5 WBC-Specific Session Handling Information

WBMC Shared will present L2TP tunnels from WBC into the CPs network to the tunnel end point as specified by:

i) the CPs RADIUS at login of each end user, OR

ii) a pre-configured list of tunnel end points associated with the Service Selection Name presented by the end users

The option to use either of these methods is selectable on a Service Selection Name (SSN) by Service Selection Name basis. Note that there is a limit of 4 CP RADIUS's per WBMC Shared Backhaul service, and a limit of 2 (Primary & Secondary) CP RADIUS servers per Service Selection Name.

4.2.5.1 WBC Session Handling under failure

If the WBMC Shared service loses all connectivity with the CPs RADIUS server then any PPP sessions with a Service Selection Name requiring communication with the CP RADIUS will be terminated within the BTW network. This feature protects the BT network from the effects of End User's equipment continuously trying to establish a PPP session and thus protects the rest of the service from a degraded performance. Similarly if WBC loses contact with the WBMC Shared proxy servers, any new PPP sessions will be terminated within the BTW network. The maximum PPP session duration associated with this feature is 10 minutes.

Where the CP has elected for the pre-configured static list of tunnel end points per Service Selection Name, if connectivity to a particular tunnel end point is lost, the WBMC Shared service will send subsequent login attempts to an alternative tunnel end point within the pre-configured list.

4.2.5.2 WBC FTTC PPP Session Timeouts

SIN 495 [16] explains that, unlike WBC ADSL end user accesses, WBC FTTC use the PPP session establishment to inform the BT Wholesale BRAS of the Openreach line rate. It is therefore essential that the PPP session is re-started every time the VDSL line retrains. To ensure this, the PPP timeout values must be set to less than 20 seconds by the CP. This is a shorter timeout than would normally be used for WBC ADSL end user sessions.

4.2.6 IPsC-Specific Session Handling Information

WBMC Shared will present L2TP tunnels from IPstream Connect into the CPs network to the tunnel end point as specified by either:

i) the CPs RADIUS at login of each end user (IPsC Session Steering), OR

ii) a pre-configured list of tunnel end points associated with the Service Selection Name presented by the end users.

4.2.6.1 IPsC Session Handling under failure

If the CPs RADIUS is used for end user authentication and/or session steering, and the WBMC Shared service loses all connectivity with the CPs RADIUS server then any PPP sessions with a Service Selection Name requiring authorisation from the CP RADIUS will be terminated within the BTW network. This feature protects the BT network from the effects of End User’s equipment continuously trying to establish a PPP session and thus protects the rest of the service from a degraded performance. The maximum PPP session duration associated with this feature is 10 minutes.

If IPsC loses contact with the WBMC Shared proxy servers & IPsC Session Steering has been selected, the IPsC RADIUS will attempt to tunnel to a set of default tunnel end points that have been pre-defined for the Service Selection Name.

If a statically pre-configured list of tunnel end points is used & connectivity to a particular tunnel end point is lost, the WBMC Shared service will send subsequent login attempts to an alternative tunnel end point within the pre-configured list.

4.3 RADIUS Interface detail

4.3.1 General

WBMC Shared provides a combined interface for both WBC and IPsC RADIUS traffic. Although WBC and IPsC are similar Broadband products, they do have key differences which will be reflected in the way the WBMC Shared to CP RADIUS interface works.

The following is a summary of the two services from a RADIUS point of view :

- Both WBMC Shared over WBC and IPsC optionally support session steering, allowing the CP to decide which LNS Tunnel End Point to use for each End User that logs on. The IPsC solution requires that all tunnelling parameters associated with a given Tunnel Server Endpoint are tagged with the same tag number (even if there is only one endpoint), whereas tagging is optional for WBC;
- Both WBC and IPsC support RADIUS Authentication of the End Users. For both, WBMC Shared will provide a Service Identifier (SID) which will allow the CP to validate the SID as part of the authentication process. The SID for WBC End Users will have a prefix 'BBEU'. The SID for IPstream Connect End Users will have the prefixes 'FTIP' or 'BBIP';
- For IPsC, it is possible to take RADIUS authentication without Session Steering. For WBC, the 2 features are linked and must be used together.
- Both WBC and IPsC support RADIUS Accounting which WBMC Shared will pass to the CP if required. IPsC Accounting packets do not require a CP RADIUS response, whereas WBC Accounting packets do require a response.

Note: The following authentication scenarios are supported for a given CP Service Selection Name:

- No RADIUS authentication interface for WBC (ADSL, FTTC, FTTP) or IPsC end users;
- A RADIUS authentication interface for WBC (ADSL, FTTC, FTTP) and IPsC end users. Tunnel session steering supported for WBC and (optionally) IPsC end users;
- A RADIUS authentication interface (including tunnel end point session steering) for WBC (ADSL,FTTC, FTTP) end users, but not for IPsC end users.

The product **does not** support the scenario where the CP requires a RADIUS authentication interface for IPsC end users but not for WBC (ADSL, FTTC, FTTP) end users on the same Service Selection Name.

CPs can elect to receive RADIUS authentication and / or accounting packets from WBMC Shared. CPs can specify up to four RADIUS IP addresses per WBMC Shared Backhaul Service which can be selected to receive authentication and / or accounting information. For each Service Selection Name, up to two RADIUS servers can be specified for Authentication, and up to two for Accounting. For both Authentication & Accounting, if two RADIUS Servers are specified, they will be treated as Primary & Secondary.

Note: If a CP has more than one WBMC Shared Service, it is possible to specify 4 different CP RADIUS server addresses for each service, and direct the RADIUS traffic to the primary RADIUS via one service and the secondary via another.

To ensure that the RADIUS traffic takes a trusted, defined route through the Backhaul to the CPs network and does not route via the internet, WBMC Shared uses NAT (network address translation) within the WBMC Shared network to translate from an IP address assigned within the WBMC Shared network to the IP address provided by the CP for their RADIUS. This NAT function happens deep within the WBMC Shared network, and once the NAT function has completed WBMC Shared will route the RADIUS packet according to the outside global and inside local NAT addresses.

CPs must ensure that they advertise their RADIUS IP address(es) to WBMC Shared via the eBGP peer over the host link(s) that they wish WBMC Shared to send the RADIUS packets. WBMC Shared will route packets via any host link that we receive a valid route over.

The CP RADIUS server(s) must be configured with all the WBMC Shared RADIUS client addresses that are applicable to all WBMC Shared interconnect nodes that the CP has service at. Failure to do this could result in RADIUS requests being ignored by the CP RADIUS server.

The CP must use RIPE addressing for their RADIUS addresses

4.3.2 Differentiating between IPsC & WBC RADIUS traffic

As mentioned above the IPsC & WBC RADIUS work differently. As WBMC is combining 2 access services, the CP needs to ensure that they handle the WBC and IPsC RADIUS interfaces appropriately.

4.3.2.1 Agnostic Approach (Recommended)

One approach is to treat all RADIUS requests the same regardless of where they originate. In this scenario, the CP does not differentiate between their responses to WBC & IPsC RADIUS requests.

For authentication requests, the CP returns the same attributes for both services, covering the required attributes of both WBC & IPsC. The solution will ensure that irrelevant attributes for WBC or IPsC are removed or do not impact the service.

For Session Steering, WBC only requires tagging of tunnel attributes in the RADIUS authentication access-accept if there is more than one Tunnel-Server-Endpoint, whereas IPsC requires tagging even if there is only one. The agnostic approach would be to always tag tunnel attributes regardless of whether the response is to WBC or IPsC.

It is important to be aware that for WBC End Users and IPsC if Session Steering has been chosen, the returned Tunnel End Point will be used by BT when setting up the tunnel to the CPs LNS. For IPsC without Session Steering the address will not be used by BT when setting up the Tunnel to the LNS – in this scenario BT will use the Tunnel End Points pre-built against the Service Selection Name in the IPsC RADIUS.

For accounting, the CP may send an accounting response for all accounting packets (as required for WBC) however since IPsC does not accept responses to accounting packets, the WBMC Shared solution will ensure accounting responses are not passed back to the IPsC RADIUS.
Note: If the customer requires IPsC Accounting packets to be sent to a Secondary RADIUS server if their Primary RADIUS doesn’t respond, the CP must respond to accounting packets to avoid receiving duplicates.

4.3.2.2 Differentiating between service types

If the CP does not wish to take an agnostic approach, there are two suggested ways of differentiating between IPsC and WBC RADIUS requests:

1) Use the Calling Station ID value in the authentication request or accounting record. This will start with “BBEU” for WBC End Users, and “FTIP” or “BBIP” for IPsC End Users;

2) For Authentication requests, act on the BT Vendor Specific Attribute of 594 which is used by the IPsC RADIUS, but not by the WBC RADIUS.

4.3.3 RADIUS Interface for WBC End Users

4.3.3.1 WBC End User Authentication and Tunnel Selection

If the CP elects to have Access Requests for some or all of their Service Selection Names proxied then the CPs RADIUS will receive messages in the following format.

The CPs RADIUS must respond with attributes from either Table 2 or 3.

No	Attribute	Value	Comment
1	User-Name	CHAP username	Name and domain as entered by End User
2	User-Password	User Password	As captured by the WBC BRAS. (See notes below)
3	CHAP-Password	User's CHAP password	As captured by the WBC BRAS. (See notes below)
4	NAS-IP-Address	BRAS source IP address	Public IP address assigned by WBMC Shared
5	NAS-Port	BRAS local port	
6	Service-Type	Framed	
7	Framed-Protocol	PPP	
31	Calling-Station-Id	End User's Line ID	As Defined by WBC - see SIN 472 [7]
32	NAS-Identifier	String	Unspecified, but unique to each WBC BRAS
33	Proxy-State	unique string	
44	Acct-Session-Id	unique string	
61	NAS-Port-Type	(5) Virtual	

Table 1 Access-Request Attributes for WBMC Shared over WBC

Note: The option specified in RFC 2865 [3], where the CHAP challenge is a 16 byte value, is used. Therefore the Access-Request authenticator contains the CHAP challenge and the CHAP-Password attribute contains the CHAP identity and response string.

Note: It is understood that WBC will support User-Password and CHAP-Password. Either User-Password or CHAP-Password will be supplied in the request, not both.

The CP RADIUS can return either an Access-Accept, or an Access-Reject in response to an Access-Request.

The set of attributes supported in an Access-Reject are shown in Table 2. A RADIUS Accounting start or stop record will not be sent in response to an Access-Reject.

No	Attribute	Value	Comment
33	Proxy-State	unique string	Exact copy of Proxy-State from the corresponding Access-Request.

Table 2 Access-Reject Attributes for WBMC Shared over WBC

The range of Access-Accept attributes supported is shown in Table 3.

No	Attribute	Value	Comment
25	Class	unique string	Optional - one or more instances
33	Proxy-State	unique string	Exact copy of Proxy-State from corresponding Access-Request.
64	Tunnel-Type	L2TP	
65	Tunnel-Medium-Type	IPv4	
67	Tunnel-Server-Endpoint	LNS IP address	(Note 1)
69	Tunnel-Password	password	Formatted to RFC2868
82	Tunnel-Assignment-ID	string	Optional
83	Tunnel-Preference	integer	Optional (Note 2)
90	Tunnel-Client-Auth-ID	string	Optional (Note 3)

Table 3 L2TP Access-Accept Attributes for WBMC Shared over WBC

Note 1: Only the dotted decimal notation format required in RFC 2868 [1] is supported. This is the IP address of an LNS within the CPs network. This must be a Public IP address.

Note 2: This attribute is used to specify the relative preference of each tunnel end point as described in RFC 2868 [1].

Note 3: The Tunnel-Client-Auth-ID is used to populate the L2TP Host Name AVP as described in RFC 2661 [2]. If the Tunnel-Client-Auth-ID attribute is not used, the default host name from the BRAS will be used. The format of this host name is unspecified but will be unique for any given BRAS.

General Note: For WBC, tagging is only required if more than one Tunnel-Server-Endpoint is used. However for consistency with IPsC, it is recommended to use tagging under all circumstances where Session Steering is being used.

Session and idle timeouts values could conceivably be returned with the L2TP attributes but this is inappropriate. If required they should be applied to an End User session on the LNS by the CP.

4.3.3.2 WBC End User RADIUS Accounting

RADIUS Accounting for WBC End Users is optional. If configured an Accounting start record is sent after an L2TP session has been established. If RADIUS accounting is enabled, CPs will also receive Interim Updates with a period of 2 hours. The list of supported Accounting attributes is shown in Table 4.

No	Attribute	Value	Comment
1	User-Name	CHAP username	Name and domain as entered by End User
4	NAS-IP-Address	BRAS source IP address	Public IP address assigned by WBMC Shared
5	NAS-Port	BRAS local port	
6	Service-Type	Framed	
7	Framed-Protocol	PPP	
8	Framed-IP-Address		Only present if session is default accepted due to CP authentication failure.
25	Class	unique string	One or more copies of Class sent in Access-Accept
27	Session-Timeout		
28	Idle-Timeout		
31	Calling-Station-Id	string	End User Line Id
32	NAS-Identifier	string	
33	Proxy-State	unique string	
40	Acct-Status-Type	Start (1) Stop (2) Interim (3) Acct-On (4) Acct-Off (5)	
41	Acct-Delay-Time		
42	Acct-Input-Octets		
43	Acct-Output-Octets		
44	Acct-Session-Id		
45	Acct-Authentic		
46	Acct-Session-Time		
47	Acct-Input-Packets		
48	Acct-Output-Packets		
49	Acct-Terminate-Cause		
52	Acct-Input-Gigawords		
53	Acct-Output-Gigawords		
55	Event-Timestamp		
61	NAS-Port-Type	Virtual (5)	

Table 4 Accounting Attributes for WBMC Shared over WBC

Accounting-Request packets must be acknowledged by an accounting response. Only a Proxy-State attribute is returned by the CP RADIUS.

No	Attribute	Value	Comment
33	Proxy-State	unique string	Exact copy of Proxy-State from the corresponding Access-Request.

Table 5 Accounting-Response Attributes for WBMC Shared over WBC

4.3.4 RADIUS Interface for IPsC End Users

IPsC support three RADIUS solutions:

- Service ID (SID) for Authentication;
- L2TP Session Steering;
- SID for Accounting.

These are options of the IPsC service. WBMC Shared CPs requiring Authentication or Accounting will be provided with the SID options. L2TP Session Steering is optional for WBMC Shared CPs taking IPsC.

Note: The IPsC SID service does not allow the use of both types of delimiter at the same time for a Domain, i.e. the @ or the / delimiter. The delimiter is the separator between the username and Domain. If you are using both types of delimiter for the Domain, you will not be able to have the SID service. When requesting the WBMC Shared service, BT will assume you are using the @ delimiter, if you are using the / delimiter please add this to the notes.

4.3.4.1 IPsC End User RADIUS Authentication

The RADIUS authentication interface for IPsC End Users is only required if the CP chooses End User Authentication and/or Session Steering. An interaction between the CP and IPsC RADIUS via the WBMC Shared RADIUS is used on each end user authentication request, with the response from the CP RADIUS determining whether the end user is given service. If required, the CP RADIUS response will also provide the Tunnel End Points.

The CP will be presented with an access request for each login attempt containing the following attributes:

No.	Attribute Name	Mandatory / Optional
1	User-Name	M
2	User-Password	M[7]
3	CHAP-Password	M[7]
4[1]	NAS-IP-Address	M
5[1]	NAS-Port	M
6	Service-Type	M
7	Framed-Protocol	M
26[2]	Vendor-Specific	M
32[3]	NAS-Identifier	M
33	Proxy-State <determined by RADIUS>	M
61	NAS-Port-Type	M
87[4]	NAS-Port-Id	M
31[5]	Calling-Station-Id	O
60[6]	CHAP-Challenge	O

Table 6 Access Request Attributes for WBMC Shared over IPsC

Notes:
1. NAS-IP-Address and NAS-Port are maintained but amended for security reasons.
2. The Customer RADIUS servers should recognise the following format and values of Vendor Specific Attribute 26 - Enterprise Code 594, Enterprise Tag 1 (containing ‘594:1:“Platform Authentication”’)
3. According to IETF RFC2865 an access request MUST contain a NAS-IP-Address (4) or a NAS-Identifier (32) or both.
4. According to IETF RFC2869 an access request should contain either a NAS-Port (5) or a NAS-Port-Id (87).
5. Attribute 31, Calling-Station-Id, will be used for populating the Service ID (SID). This field will take the form “FTIP<numeric>” or “BBIP<numeric>” in some instances the SID may be post fixed by a sequence containing a port ID in which case the attribute will take the form of “FTIP<numeric>:IPIA<numeric>” or BBIP<numeric>:IPIA<numeric>”. The SID is the end user identifier used in the IPstream provision, reporting and Advanced Services interfaces.

6. Attribute 60, CHAP-Challenge may be populated for requests depending on the source equipment within BT Wholesales platform.

7. Either User-Password or CHAP-Password will be supplied in the request, not both

The CP RADIUS is required to respond with an access accept message as follows:

No.	Attribute Name	Attribute Content	Mandatory/Optional/ Alternate
6	Service-Type	Framed	M
7	Framed-Protocol	PPP	M
8	Framed-IP-Address[1]	IP address to be used by the end-user	O
22	Framed-Route[1]	Used for No_NAT routing updates	O
33	Proxy-State	<determined by RADIUS>	O
25	Class	<string> to appear in all Accounting-Requests associated with the session	O
26	Vendor Specific Attribute	Juniper Context-Name VSA. Required for all End User Session Steering Requests. Normally set to 4874:1:"central"	M[7]
67	Tunnel-Server-Endpoint[2]	CP LNS IP address	M[7]
64	Tunnel-Type	L2TP	M[7]
65	Tunnel-Medium-Type	IPv4	M[7]
69	Tunnel-Password[3]	Password	M[7]
82	Tunnel-Assignment-ID	String	O
83	Tunnel-Preference[4]	Preference for the associated Tunnel-End-Point	M[7]
90	Tunnel-Client-Auth-ID[5]	String	M[7]

Table 7 Access Accept Attributes for WBMC Shared over IPsC

Notes:

1. For SID for Authentication, without session steering, Framed-Route or Framed-IP-Address must be returned. This drives the BT Wholesale RADIUS to tunnel the end user's PPP session to a pre-defined tunnel end point associated with the service selection name presented by the end user during the PPP session setup attempt. For Session Steering, these parameters need not be sent to drive tunnelling of the session. If they are sent, they will be ignored by BT RADIUS. If the CP does not require Session Steering and responds but leaves attributes 8 and 22 blank, then the end user's PPP session will be terminated within BTW's network and the End User will not receive service.
2. The Tunnel-Server-Endpoint is the IP address of an LNS within the CPs network. This must be a Public IP address. IP Addresses must be in dotted decimal format as specified in RFC 2868 [1].
3. Tunnel-Password must be formatted to RFC2868
4. Tunnel-Preference is mandatory. If a CP has a preference, the Tunnel Server Endpoint with the lowest preference value (e.g. 1) will be given first preference. If a CP doesn't wish to specify a preference, the same value should be used for all Tunnel Server Endpoints.
5. The Tunnel-Client-Auth-ID's returned by a CP may be different for each response; however they must be the same for all tunnels that are destined for a given Tunnel Server Endpoint IP Address.
6. Any tunnelling parameters received other than those listed in the table above will be filtered out by BT RADIUS.
7. Tunnelling Parameters are only mandatory if the CP has chosen the Session Steering option.

The IPsC session steering functionality supports multiple Tunnel-Server-Endpoints for each Access-Accept. However in order to avoid performance issues, it is strongly recommended that no more than 3 tunnel end points are returned per end user access accept.

The customer RADIUS must support tagging. All tunnelling parameters associated with a given Tunnel Server Endpoint must be tagged with the same tag number. For IPsC, if a CP only returns one Tunnel Server Endpoint, it must still be tagged.

If the CP does not wish the End User to have service, an Access Reject should be sent in response. The proxy-state attribute may be returned in the Access Reject message. No other attributes are required.

4.3.4.2 IPsC End User RADIUS Accounting

The CP can opt for RADIUS accounting for their IPsC End Users. This is in addition to any RADIUS accounting options that the CP may implement in their own network e.g. on their LNS.

The RADIUS accounting data transfer attributes (42, 43, 47 and 48) have a level of accuracy comparable with typical IP traffic measurement equipment. However there are circumstances under which accounting packets and records may be lost. The traffic measurements are therefore an approximate indication of the individual end user traffic.

The format of the RADIUS accounting data generated by BTW is as specified in the following table:

Attribute	Value	Type of Value	Start	Interim[5] (Option)	Stop
User-Name	1	string	✓	✓	✓
NAS-IP-Address[1]	4	integer	✓	✓	✓
NAS-Port[1]	5	integer	✓	✓	✓
Service-Type	6	integer	✓	✓	✓
Framed-Protocol	7	integer	✓	✓	✓
Framed-IP-Address[2]	8	integer	✓	✓	✓
Class[3]	25	string	✓	✓	✓
Calling-Station-ID[4]	31	string	✓	✓	✓
Proxy-State	33	string	✓	✓	✓
Acct-Status-Type	40	integer	✓	✓	✓
Acct-Delay-Time	41	integer	✓	✓	✓
Acct-Input-Octets	42	integer		✓	✓
Acct-Output-Octets	43	integer		✓	✓
Acct-Session-Id	44	string	✓	✓	✓
Acct-Authentic	45	integer	✓	✓	✓
Acct-Session-Time	46	integer		✓	✓
Acct-Input-Packets	47	integer		✓	✓
Acct-Output-Packets	48	integer		✓	✓
Acct-Terminate-Cause	49	integer			✓
Acct-Input-Gigawords	52	integer		✓	✓
Acct-Output-Gigawords	53	integer		✓	✓
NAS-Port-Type	61	integer	✓	✓	✓

Table 8 RADIUS Accounting Attributes for WBMC Shared over IPsC

Notes:

1. NAS-IP-Address and NAS-Port are maintained but amended for security reasons.
2. Framed-IP-Address (Attribute 8) is only present in Accounting for PTA Mode End Users.
3. a) It is possible to have multiple Class attributes in accounting requests.
   b) Currently the IPstream Connect service does not support the presence of a null (hex 00) in the Class Attribute (attribute 25) string. If a null is used in attribute 25 in the access-accept, the string that appears in the accounting requests for the session may be truncated at the null.
4. The CP will be presented with the SID of the end user in attribute 31 (Calling-Station-Id) for each accounting packet. This field will take the form "FTIP<numeric>" or "BBIP<numeric>". The SID is the end user identifier used in the IPstream Connect provision, reporting and Advanced Services interfaces.
5. The interim accounting period is two hours.

4.4 WBMC Shared Traffic Types

WBMC Shared currently supports WBC Best Efforts (Priority, Best and Sub), WBC Real Time and IPsC Best Efforts traffic.

The following table summarises the traffic classes supported by WBMC Shared.

Product	**Class**	**DSCP codepoint (IETF)**	**Binary value**	**Decimal value**
WBC	**Real-time (RT)**	**EF**	**101 110**	**46**
WBC	**Priority Best Effort**	**AF21**	**010 010**	**18**
WBC	**Standard Best Effort (SBE)**	**Default**	**000 000**	**0**
WBC	**Sub Best Effort**	**EXP/LU**	**000 011**	**3**
IPsC	**Best Effort (BE)**	**Default**	**000 000**	**0**

Table 9 DSCP Markings

WBMC Shared's handling of traffic will be as follows:

- The CP purchases (from WBMC Shared) independent amounts of IPsC Best Efforts (BE) and WBC Total BE traffic. WBC Real Time traffic is not purchased – the CP can use up to 5% of the physical bandwidth on a link for Real Time traffic. Above 5% the Real Time traffic will be policed & dropped.

- Other than WBC Real Time traffic, WBMC Shared will only police traffic once it reaches the physical limits of the links.

- Burst bandwidth will be calculated based on the combined WBC & IPsC Best Efforts traffic counted on the CPs service.
- To avoid burst charges, CPs should manage their traffic into WBMC to ensure they do not exceed their contracted bandwidth (for Best Efforts) or the 5% limit for Real Time QoS bandwidth.
- Traffic for all WBC End User Access technologies is classed as WBC traffic; it is not marked or counted differently for each technology.

- Other QoS Markings besides those stated in Table 9 are treated as BE.

- CPs are advised to re-mark any EF marked traffic which is not associated with a WBC end user access with RTQoS enabled to ensure that RTQoS bandwidth is available for valid RTQoS end users.

  Note: It is recommended that L2TP control traffic is prioritised by the CPs LNS and that CPs shape or police their own traffic before handover to WBMC. Excess traffic (above the physical limit of the link) will be policed on ingress by WBMC. As L2TP and PPP control traffic have no special status at the ingress policer, there is a risk that the L2TP tunnel will be dropped under severe and prolonged congestion. This will result in end user sessions on that tunnel being terminated and the end users having to start a new PPP session.
- On the WBMC Shared network, WBC Priority Best Efforts and Sub Best Efforts will be treated in the same way as standard WBC Best Efforts traffic.

The total of the bandwidth of all traffic classes cannot exceed the amount of bandwidth that can be supported by the physical Host Links ordered by the CP.

Notes:

1) WBMC Shared does not act upon the DSCP marking of IP packets carried by PPP sessions within the L2TP tunnels carried by WBMC Shared. Current information from WBC & IPsC indicates that they also only act upon the outer (L2TP carrying) DSCP marking (for both AP measurement and policing and BRAS Queuing).

5 References

Reference Number	Document Title
1	RFC2868 RADIUS Attributes for Tunnel Protocol Support
2	RFC2661 Layer Two Tunnelling Protocol “L2TP”
3	RFC2865 Remote Authentication Dial In User Service (RADIUS)
4	RFC2869 RADIUS Extensions
5	[Removed]

6	[Removed]	
7	SIN 472	BT Wholesale Broadband Connect (WBC) Products, Service Description
8	SIN 477	FTTP Generic Ethernet Access Service & Interface Description
9	SIN 482	BT IPstream Connect Service Description
10	[Removed]	
11	SIN 485	BT IPstream Connect Office, BT IPstream Connect Home, BT IPstream Connect Max & BT IPstream Connect Max Premium Products, Service Description
13	[Removed]	
14	SIN 487	BT IPstream Connect Symmetric, Service Description and Interface Specification
15	SIN 492	Ethernet Access Direct (EAD) and Ethernet Access Direct Local Access, Service & Interface Description
16	SIN 495	BT Wholesale Broadband Connect Fibre to the Cabinet, Service Description
17	SIN 496	BT IPstream Connect SID for Authentication, Service & Interface Description
18	SIN 497	BT IPstream Connect SID for Accounting, Service & Interface Description
19	SIN 498	Fibre to the Cabinet (FTTC) Generic Ethernet Access Service and Interface Description
20	SIN 502	BT IPstream Connect Session Steering, Service and Interface Description
21	SIN 506	Fibre to the Premises (FTTP) Generic Ethernet Access, Service and Interface Description
22	SIN 509	BT Wholesale Broadband Connect (WBC) Fibre to the Premise (FTTP), Service & Interface Description
23	SIN 519	Ethernet Access Direct (EAD) 10000, Service & Interface Description

6 Abbreviations

AC	Alternating Current
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding

AP	Aggregation Point
AR	Assured Rate
AS	Autonomous System
ATM	Asynchronous Transfer Mode
AVP	Attribute-Value Pair
BAS	Broadband Access Server
BBCR	Broadband Customer Reporting
BBIP	Broadband IP service identifier
BC	Business Customer
BE	Best Effort
BRAS	Broadband Remote Access Server
BTW	BT Wholesale
CHAP	Challenge Handshake Authentication Protocol
CP	Communications Provider
CRF	Customer Requirement Form
DSCP	Differentiated Services Code Point (IETF)
DSLAM	Digital Subscriber Line Access Multiplexer
DWDM	Dense Wavelength Division Multiplexing
EAD	Ethernet Access Direct
eBGP	External Border Gateway Protocol
EF	Expedited Forwarding
EU	End User
FER	Front End Router
FTIP	IP service identifier
FTTC	Fibre to the Cabinet
FTTP	Fibre to the Premise
Gbps	Gigabits per second
GEA	Openreach Generic Ethernet Access product
IEEE	Institute of Electronic and Electrical Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4 [IETF]
IPR	Intellectual Property Rights
IPsC	IPstream Connect

ISP	Internet Service Provider
L2	Layer 2
L2TP	Layer 2 Tunnelling Protocol
L3	Layer 3
LAC	L2TP Access Concentrator (function in BAS)
LAN	Local Area Network
LNS	L2TP Network Server (e.g. Home Gateway)
Mbps	Megabits per second
MED	Multi-Exit Discriminator
MPLS	Multi-Protocol Label Switching [IETF]
MSAN	Multi-Service Access Node
MSE	Multi-Service Edge
MSIL	Multi-Service Interconnect Link
MTU	Maximum Transmission Unit
NAT	Network Address Translation
no NAT	Optional removal of NAT for Static IP Addressing
NTE	Network Termination Equipment
PC	Personal Computer
PPP	Point to Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
RT	Real Time
SID	Service Identifier
SINs	Suppliers' Information Notes
SMPF	Shared Metallic Path Facility
SOGEA	Single Order Generic Ethernet Access
SP	Service Provider
SSN	Service Selection Name
TCP/IP	Transmission Control Protocol/ Internet Protocol
VDSL	Very high speed Digital Subscriber Line

VLAN	Virtual LAN
WBC	Wholesale Broadband Connect
WBMC	Wholesale Broadband Managed Connect

7 History

Issue	Date	Changes
Issue 1.0	6 Jun 2008	First Issue
Issue 1.1	20 Mar 2009	Removed references to an optional MSIL delivery mechanism (incl amendment to Figure 2), which was not implemented. Clarified the current and future availabilities of speeds at and above 8Gbps. Also minor editorials.
Issue 1.2	31 Jul 2009	Table 3 Note 1 updated to specify that the Tunnel endpoint IP address (the LNS) must now be a Public IP address
Issue 1.3	5 Aug 2009	Introduction updated to reference STIN499. Also Section 4.2.2 (Connectivity to the CPs network and Routing updates) amended to specify that only public IP address ranges should be associated with each eBGP peer
Issue 1.4	2 Sep 2009	Noted that BT plans to launch WBMC Shared consuming IPstream Connect on 30th September 2009. Full details are currently at STIN499 but will be incorporated into SIN 471 before 30th September 2009.
Issue 2.0	14 Sep 2009	SIN updated to introduce WBMC consuming IPstream Connect
Issue 2.1	5 Nov 2009	4.2 & 4.4 - Changes to introduce Burst Bandwidth & Bandwidth Cap 4.2.2 – Clarified WES termination & the need for 2 RIPE /30 addresses per resilient host link; Identified the need for 16 bit AS Numbers 4.2.3 – Clarified use of the same SSN on WBC & IPSC and maximum SSNs per CP 4.2.4 & 4.3.1 – Clarified the limits of CP RADIUS servers per WBMC Service and per SSN 4.3.2.1 – Clarified the use of Primary/Secondary servers for Accounting

		4.3.4.2 – Modified IPSC Accounting attributes to align with v1.5 of SIN482 General – minor wording clarifications
Issue 2.2	26 Nov 2009	Sections 2, 4.1 & 4.2.2 - Document modified to reflect introduction of EAD in place of WES for new host link orders. General – minor editorials.
Issue 2.3	21st Jan 2010	General - Updated to cover the introduction of WBMC over WBC FTTC End User Access. Section 1 - Clarified the list of WBC & IPsC SINs Section 4.2.2 – Clarified the need for Public AS Numbers Section 4.3.4.1 - Modified the Access-Accept parameters General - minor editorials.
Issue 3.0	May 2011	General – Updated to reflect the introduction of 10G Host Links 3. – Included a reference to ADSL2+ Annex M 4.2.2 – Clarified the need to advise BT of the prefixes that will be advertised; clarified that MEDs only work across host links on one service instance; clarified how BRAS tunnel end point addresses are advertised; Modified wording to include support for Private AS numbers 4.2.3.3 – Removed Domain Nameless option since no longer supported 4.4 – Clarification of L2TP control packet handling
Issue 3.1	November 2011	Sections 1., 4.2.5, 4.3.1, 4.3.2, 4.3.4, - Introduction of IPsC Session Steering Sections 4.2.1, 4.4 – Introduction of WBC Real Time QoS General – Added in references to WBC Fibre to the Premise Section 4.2.2 – Clarification on growth of tunnel end points, AVP24/38 limitation and additional AS number for the WBC MSE Section 4.2.4.1 – Clarification of WBC failure handling

		Section 4.3.3 – Clarification of tunnel preference and tagging Section 4.3.4.1 – Removed Filter-id attribute from IPsC Access Accept Section 4.4 – Added WBC Priority and Sub Best Efforts traffic Added a References section
Issue 3.2	July 2013	Section 4.2.2 – Added a statement on MTU Size; Removed the WBC MSE AVP24/38 limitation
Issue 3.3	January 2014	Section 4.2.1 – Updated to reflect that Real Time QoS is supported for FTTC/FTTP Section 4.2.2 – Added a statement on AS Paths. Section 4.2.3.2 – Added guidance to the limit of Service Selection Names per CP. Section 4.2.3.3 - Added '$' to the list of reserved characters.
Issue 3.4	August 2014	Section 2 & 4.3.1 – Changes to align with the introduction of Metro Node Connectivity Section 4.2.3 – Added a new sub-section covering guidelines on AS Numbers, including guidelines for AS Numbers & Metro Node Connectivity General – Minor editorial & formatting changes Change SINet site references from http://www.sinet.bt.com to http://www.btplc.com/sinet/
Issue 3.5	July 2015	Section 1. & 2. – Updated the links to BT Wholesale and Openreach websites Section 1., 5. – Removed references to obsolete Assured Service SINs Section 2., 4.1 & 4.2.2 - Changes to reflect the introduction of Datacentre (Telehouse) handover. Section 4.3.3.1 – Corrected the note on CHAP Challenge from 16 bits to 16 bytes.
Issue 3.6	August 2016	Section 2, 3, 4.1, 4.2.2. – Changes to reflect the introduction of In Building Handover Section 2, 4.1, 4.2.2, 5. – Introduction of 10G EAD in place of 10G WES for new Customer Sited Handover orders

Issue 3.7	July 2019	4.2.1 changes to define the updated working of RTQoS (upstream and downstream) and revised policing approach for RTQoS bandwidth 4.4 updates to clarify the updated working of RTQoS.
Issue 3.8	June 2020	General – removal of "burst cap" option which was previously supported for 1G services 4.1 changes to recommend CPs don't mix 1G and 10G Host Links. 4.2.1 – changes to reflect the changed way of handling contracted bandwidth and bandwidth policing. 4.2.2 – Tidy up of wording around WES/EAD, change of IP addressing example to use public rather that private addresses, changed prefix limit from 384 to 400, added a note that routing decisions are not based on AS path length, revised statement on number of tunnel end point IP addresses 4.2.3 – changed to reflect support for 32 bit AS numbers 4.3.1 – updates to reflect changes in advertising of CP RADIUS IP addresses 4.4 – Changes to rules associated with traffic types.
Issue 3.9	February 2021	General updates to: • Removed references to Openreach WES throughout the document. • Include WBC SOGEA end user access • Replaced CP's with CPs throughout the document. 2. Updated to reflect 100G Host Link availability 4. Clarification that recommends against mixing 1G, 10G and 100G Host Links at the same interconnect node. 4.2.3 Clarification on AS Numbers to confirm the same AS Number can be used on multiple service instances at an interconnect node.
Issue 3.10	July 2023	General updates to:

		- Include mention of SOADSL / SOTAP as a valid WBC product option - Update diagrams of WBMC interconnect with WBC to remove MSIL as MSIL no longer used

<END>